



Department of Defense

DIRECTIVE

NUMBER 5200.39

September 10, 1997

ASD(C3I)

SUBJECT: Security, Intelligence, and Counterintelligence Support to Acquisition
Program Protection

References: (a) DoD Directive 5000.1, "Defense Acquisition," March 15, 1996
(b) DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," March 1996
(c) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988
(d) DoD 5200.1-M, "Acquisition Systems Protection Program," March 1994
(e) through (p), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities to security, intelligence, and counterintelligence (CI) activities that provide support to acquisition organizations after critical acquisition program information, technologies, and/or systems have been identified. Such information is hereafter referred to as critical program information (CPI). CPI requires protection to prevent its unauthorized or inadvertent disclosure, or loss (hereafter referred to as "compromise").

1.2. Provides specific assignments of responsibility and is intended to supplement references (a), (b), and (c).

1.3. Continues to authorize publication of reference (d), in accordance with DoD 5025.1-M (reference (e)).

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

4.1. It is DoD policy to provide protection for CPI that, if compromised, would significantly alter program direction; compromise the program or system capabilities; shorten the expected combat-effective life of the system; or require additional research, development, test, and evaluation resources to counter the impact of CPI compromise. CPI shall be identified early in the acquisition life cycle (not later than Milestone I or when the program enters the acquisition process) by the acquisition Program Manager (PM) and shall be protected.

4.2. Working together, acquisition, security, intelligence, and CI organizations shall recommend protective measures for CPI in order to protect the acquisition program's technological lead. Acquisition organizations shall identify CPI and provide program goals and objectives to the security, CI, and intelligence organizations. CI and intelligence organizations shall provide assessments of collection capabilities and potential threats from foreign interests to acquisition programs. Security organizations shall identify system vulnerabilities and shall recommend cost-effective security measures using risk management evaluations. CI organizations may conduct operations necessary to counter threats to those programs. Information gathered by the DoD intelligence community must comply with DoD Directive 5240.1 (reference (f)) and DoD 5240.1-R (reference (g)). Information gathered by non-intelligence community entities must comply with DoD Directive 5200.27 (reference (h)).

4.3. General

4.3.1. When designated a DoD acquisition program, that program, to include documentation, technologies, and system hardware, shall be reviewed by the PM to identify CPI.

4.3.2. When a program does contain CPI, whether it be integral to that program, inherited from another program, or result from non-traditional acquisition

techniques (e.g., Advanced Concept Technology Demonstration, flexible technology insertion), a Program Protection Plan (PPP) shall be developed as described in DoD 5200.1-M (reference (d)), approved by the PM, and reviewed by the Milestone Decision Authority (MDA).

4.3.3. If the PM determines that there is no CPI associated with the program (neither integral to the program nor inherited from a supporting program), a PPP is not required. The PM shall make this determination in writing for review by the MDA.

4.3.4. When a program contains CPI, multi-disciplinary threat, vulnerability, and risk assessments shall be conducted to determine the threat against that information. These assessments shall provide the basis for risk management decisions and for identification of appropriate cost-effective security countermeasures required to negate the threat.

4.3.5. Program protective measures shall be applied at all locations where CPI is developed, produced, analyzed, tested, maintained, transported, stored, or used in training.

4.3.6. Incidents of loss, compromise, or theft of identified CPI shall be reported in accordance with procedures in DoD Instruction 5240.4 (reference (i)) and DoD 5200.1-R (reference (j)), as appropriate.

4.4. Program Protection Planning Process

4.4.1. The objective of effective program protection planning is to prevent exploitation of U.S. technology or the development of countermeasures against U.S. defense systems. The goal is to selectively and effectively apply security countermeasures that are cost-effective and consistent with risk management principles.

4.4.2. Guidance for developing a PPP, as well as a description of these elements, is contained in the Defense Acquisition Deskbook and DoD 5200.1-M (reference (d)). A PPP shall address at a minimum the following elements:

4.4.2.1. System and Program Description.

4.4.2.2. List of CPI to be protected in the system or program.

4.4.2.3. Threats to CPI.

4.4.2.4. Vulnerabilities of CPI to threats.

4.4.2.5. Technology Assessment and Control Plan.

4.4.2.6. Classification Guides.

4.4.2.7. Countermeasures.

4.4.2.8. Protection costs.

4.4.2.9. Foreign Disclosure.

4.4.2.10. Foreign Sales and Co-Production.

4.4.2.11. Follow-on Support.

4.5. Integrated Product Team (IPT) Process. Using the IPT process, representatives of appropriate offices or organizations responsible for the elements listed in subparagraph 4.4.2., above, shall participate in developing a program-specific PPP. Guidance for using or convening a Security IPT or security element of a program IPT is contained in reference (d) and the Defense Acquisition Deskbook.

4.6. Horizontal Protection. Common security countermeasures for protecting similar technologies shall be used by acquisition programs and the DoD Components. Officials with responsibilities listed in this Directive shall assess their programs and implement protective actions to ensure the cost-effective application of program protection efforts.

4.7. Training. DoD training programs for acquisition, security, and CI personnel shall include training on implementation of acquisition program protection and risk management.

4.8. Special Access Programs (SAPs). The unique nature of SAPs requires compliance with special security procedures of DoD Directive O-5205.7 (reference (k)). Security, intelligence, and CI organizations shall assist SAP PMs in developing a comprehensive plan for protecting CPI if the acquisition program transitions to a collateral or unclassified status. The plan will be provided to the offices responsible for implementing protection requirements before beginning the transition.

4.9. Waivers and Exceptions. The DoD Components have no authority to waive or exempt the requirements of this Directive.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Acquisition and Technology shall:

5.1.1. Provide day-to-day direction and management for acquisition program protection in accordance with DoD Directive 5200.1 (reference (l)), and may delegate authority to the DoD Component Acquisition Executives to:

5.1.1.1. Ensure acquisition PMs review their program to identify CPI, and designate an appropriate staff office to ensure that a PPP is developed when necessary.

5.1.1.2. Ensure that CPI is appropriately protected.

5.1.1.3. Plan and program fiscal resources to identify and protect CPI.

5.1.1.4. When a prime contractor or subcontractor is to have access to CPI, ensure that all prime contracts and subcontracts:

5.1.1.4.1. Identify the CPI.

5.1.1.4.2. Describe specific countermeasures to protect CPI that the baseline National Industrial Security Program lacks.

5.1.1.4.3. Authorize access to contractor facilities, by the Defense Investigative Service (DIS) or other cognizant security authority, to permit surveys, inspections, or inquiries necessary to assure implementation of program protection activities.

5.1.1.5. Ensure appropriate training is conducted for personnel responsible for assisting in the preparation and implementation of protection requirements set forth in PPP documents.

5.1.1.6. Ensure program protection issues are addressed in the IPT process for appropriate resolution.

5.1.2. Delegate authority to the Director, Special Programs, to ensure that CPI is properly protected if a program transitions from special access to collateral or unclassified status.

5.1.3. Develop procedures to resolve differences between programs in identifying and protecting CPI.

5.1.4. Support development and implementation of a horizontal protection system for data exchanged between programs.

5.1.5. Ensure the Director, On-Site Inspection Agency, as the Executive Agent for the Defense Treaty Inspection Readiness Program:

5.1.5.1. Provides arms control and/or counter-proliferation security assessments for appropriate treaties and executive agreements.

5.1.5.2. Participates in the IPT process, as it relates to horizontal protection, to assist in developing program-specific PPPs.

5.2. The Under Secretary of Defense for Policy shall:

5.2.1. Share appropriate information in security policy automated databases with organizations responsible for program protection.

5.2.2. Negotiate, coordinate, review, and approve necessary security arrangements with other governments, as appropriate, in accordance with DoD Directive 5230.11 (reference (m)), DoD Directive 5230.20 (reference (n)), and DoD Directive 2040.2 (reference (o)).

5.2.3. Provide guidance to the DoD Components on security arrangements for international programs, including participation in related IPTs.

5.3. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall:

5.3.1. Establish security policy and provide technical security assistance for acquisition program protection.

5.3.2. Establish and manage a system to provide horizontal protection, including associated automation support.

5.3.3. Serve as the DoD-level focal point for Federal Agencies outside the Department of Defense that provide assistance in protecting CPI.

5.3.4. Participate in the IPT process, as it relates to acquisition program protection, to support the DoD Component Head, Acquisition Executive, or other Milestone Decision Authority.

5.3.5. Participate in the Defense Acquisition Board and Overarching Integrated Product Teams for Major Defense Acquisition Programs and Major Automated Information System acquisition programs.

5.3.6. Oversee the process used by the DoD Components for acquisition program protection.

5.3.7. Provide resources necessary to support the development of program protection training.

5.3.8. Ensure the Director, Defense Intelligence Agency:

5.3.8.1. Provides technology targeting assessments detailing specific intelligence collection capabilities or other threats from foreign interests. These assessments, updated as required, will include an analysis of the forecasted needs of foreign interests for specific DoD technologies and information.

5.3.8.2. Provides technology transfer risk assessments for technologies and foreign interests of concern.

5.3.9. Ensure the Director, DIS:

5.3.9.1. Conducts reviews, as well as advice and assistance visits, of contractor facilities within the United States to assess compliance with contractually imposed program protection countermeasures, for both classified and unclassified CPI, when contract provisions authorize.

5.3.9.2. Participates in conducting surveys at contractor facilities to support program protection requirements.

5.3.9.3. Provides relevant threat information, when available and authorized for release, to contractors having access to CPI.

5.3.9.4. Provides industrial security support to the IPT process.

5.3.9.5. Directs the Director, DoD Security Institute, to develop and conduct training for program protection.

5.4. The Inspector General of the Department of Defense shall ensure that the DoD Components that are not members of the Intelligence Community comply with DoD Directive 5200.27 (reference (h)) when providing support to acquisition program protection.

5.5. The Assistant to the Secretary of Defense for Intelligence Oversight shall ensure that Defense Intelligence Components comply with DoD Directive 5240.1 (reference (f)) and DoD 5240.1-R (reference (g)) when providing support under this Directive.

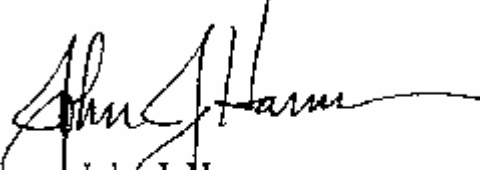
5.6. The Heads of the DoD Components shall:

5.6.1. Provide intelligence threat assessment support required for each acquisition program managed by the DoD Component and, to the maximum extent possible, make threat information available to contractors with access to CPI.

5.6.2. Provide CI and security support to the IPT process, when appropriate.

6. EFFECTIVE DATE

This Directive is effective immediately.



John J. Hamre
Deputy Secretary of Defense

Enclosures - 2

- E1. References, continued
- E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD 5025.1-M, "DoD Directives System Procedures," August 1994
- (f) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988
- (g) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that affect United States Persons," December 1982
- (h) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
- (i) DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," September 22, 1992
- (j) DoD 5200.1-R, "Information Security Program Regulation," January 1997
- (k) DoD Directive O-5205.7, "Special Access Program (SAP) Policy," January 13, 1997
- (l) DoD Directive 5200.1, "DoD Information Security Program," January 17, 1997
- (m) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (n) DoD Directive 5230.20, "Visits and Assignments of Foreign Representatives," April 24, 1992
- (o) DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984
- (p) DoD Directive 5530.3, "International Agreements," June 11, 1987

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Acquisition Program. A directed, funded effort that is designed to provide a new, improved, or continuing weapons system or automated information system capability in response to a validated operational need. Acquisition programs are divided into categories, which are established to facilitate decentralized decision-making and execution and compliance with statutory requirements.

E2.1.2. Critical Program Information (CPI) (formerly, Essential Program Information, Technologies, and/or Systems). Critical program information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such programs, technologies, or systems.

E2.1.3. Foreign Interest. Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the law of any country other than the United States or its possessions and trust territories; and any person who is not a citizen or national of the United States.

E2.1.4. Horizontal Protection. The process that ensures CPI associated with more than one acquisition program is protected to the same degree by all involved DoD Components.

E2.1.5. Program Protection Plan (PPP). A comprehensive plan to safeguard critical program and technology information that is associated with a defense acquisition program. The level of detail and complexity of the PPP will vary based on the criticality of the program or system, the CPI, and the phase of the acquisition process being addressed.

E2.1.6. Risk Management. An organized, analytical process of identifying vulnerabilities, quantifying and assessing associated risks, and implementing and/or controlling the appropriate approach for preventing or handling each risk identified.

E2.1.7. Technology Assessment and Control Plan. The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and, the development of access controls and measures necessary to protect the U.S. technological or operational advantage of the system, as prescribed in DoD Directive 5230.11 (reference (m)) and DoD Directive 5530.3 (reference (p)).